भारत सरकार
GOVERNMENT OF INDIA

लद्दाख का राजपत्र
The Ladakh Gazette

एस.जी.-एल.डी.-अ.-01082024-1344
SG-LD-E-01082024-1344

असाधारण
EXTRAORDINARY
प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

लद्दाख, 01 अगस्त, 2024
LADAKH, THURSDAY, AUGUST, 01, 2024

Part II - Section 3

केन्द्र-शासित प्रदेश लद्दाख प्रशासन
ADMINISTRATION OF UNION TERRITORY OF LADAKH

Information & Cyber Security Policy, UT Ladakh 2024

INFORMATION TECHNOLOGY DEPARTMENT

NOTIFICATION

In spite of an elaborate information and cyber security ecosystem set forward for India, the number of cyber incidents has only been on the rise since then. With countless sectors now shifting to digital platforms, there has been a humongous increase in the amount of data generated as a result. The pace at which data is being generated has not been matched with the enforcement of security standards to protect it, which has resulted in a drastic increase in cyber-attacks in India in the past decade. Cyberspace is vulnerable to a wide variety of incidents like identity theft, phishing, social engineering, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates. Cyber incidents have the potential to cause complications that may threaten individual lives, economy of the state and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. Further protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

The UT Administration of Ladakh to stay focused on establishing strong practices in governance, automation and digitalization, has developed this Information and Cyber Security Policy (ICSP) to ensure security of Critical Information Infrastructure (CII) and other IT resources provided to its employees to ensure the safety, security, privacy and protection of the employees and the information assets they engage with on a day-to-day basis.

These CII and IT resources need a policy framework to ensure continued availability to access and process information related to their areas of work. The Government officials are enabled and well informed to carry out their functions in an efficient and effective manner when the tools and infrastructure are protected and accessed in a disciplined manner by the users of data and Information assets.

For the purpose of this policy, the term 'CII and other IT Resources' includes desktop devices, portable and mobile devices, networks including wireless networks, internet connectivity, storage devices and peripherals like printers and scanners and applications and software associated therewith.

To avoid misuse of CII and IT resources this policy puts in place a framework to guide and advice the UT Administration to manage its information assets and users and help them in exercising caution and take a disciplined approach to avoid unwanted risks and liabilities that can pose threat for the Government infrastructure and create hurdles and delays in its functioning.

Accordingly, this ICSP when effectively deployed ensures that the information assets and critical information infrastructure resources are identified, managed, and handled using authenticated access protocols in lawful and ethical ways for purposes that the UT Administration of Ladakh may engage in.

1. The Vision Statement

The Information and Cyber Security Policy Vision of the UT Administration of Ladakh is:

"to create a safe cyber space that protects its critical information infrastructure, IT resources and data to allow its citizens to safeguard their privacy, enable businesses to safely interact and transact and empower government departments in delivering undisrupted services in a stable and secure environment."

The ICSP of the UT of Ladakh shall be compliant to the legal requirements and regulatory framework while serving and extending the services to the people of the UT of Ladakh and the Union of India. The primary goal would be to protect the CII and IT applications used by government departments and institutions. The ICSP framework aims at proactively establishing the required controls to mitigate the vulnerabilities, threats, and risks to its assets by identifying, analyzing, resolving, and mitigating, periodically monitoring, and managing the information security vulnerabilities, threats, and risks in order to protect its IT Infrastructure covering its IT assets, information and data. The focus will also be on integrating the criteria and assertions for protecting the IT assets and establishing a strong Information security framework. The robustness of the security framework will be reinforced through of identification and elimination of the vulnerabilities, laying strong emphasis on the resilience, continuous monitoring, and continuous improvement in the information security to proactively stay alert to the evolving and emerging information security threats. This will be achieved by

1. ***Incorporating the information security framework***: Incorporating the information security framework with the administrative, operational, technical, and assurance activities by integrating and carefully sequencing the information security tasks with the business processes and services of the UT Administration of Ladakh and its functions, departments, consultants, employees, partners, affiliates,

enterprises, and retainers.

2. ***Secure Service Delivery***: Building familiarity and increasing the efficiency to provide secure service delivery through awareness building amongst the employees of the establishment, its functions, departments, affiliates, personnel, consultants, and retainers, on this policy, the principles and guidelines governed by this policy.
3. ***Establishing process controls***: Establishing the process controls to protect information and data assets including electronic and personal data, of the Government across the UT.
4. ***Identifying risk & vulnerabilities***: Identifying the risk and vulnerabilities associated with the second party and third-party service providers and mitigating the same through effective rules of engagement confirming to confidentiality, completeness, accuracy, availability and integrity, materiality, reliability, efficiency and effectiveness and compliance to the data protection and privacy requirements.
5. ***Effective deployment***: Ensuring that the rules of engagement are applicable not just during the period of service provision but for a time period into the future until which the impact of a vulnerability can be felt.
6. ***Continuous improvement***: Continuing the improvements in the risk and vulnerability management and mitigation, strengthening the applicable controls from time to time with sophistication and robustness and addressing emerging challenges and threats that arise from the cyber world.

2. The ICS Policy Mission

The Information and Cyber Security Policy Mission envisaged by the UT Administrationof Ladakh translates into achieving the following components.

- Establish mechanisms and controls through ICSP that shall engage in identifying, analysing, resolving, and mitigating any vulnerabilities, threats and risks caused by cyber threats.
- Establish robust IT systems by identifying and eliminating all vulnerabilities, by laying strong emphasis on cyber resilience and business continuity, continuous monitoring and continuous improvement.
- Establish guidelines for developing Standard Operating Procedures (SOPs) in government departments to protect its CII, IT resources, information and data through periodic monitoring and information security management.
- Establish appropriate institutional arrangements and delineating their roles and responsibilities including ownership and security of the CII and IT resources used by each organization, department, function operating in the UT of Ladakh.
- Establish capacities that would enable the UT Administrationof Ladakh to create an informed and competent workforce and create a cadre of officers with expertise in information and cyber crisis management.
- Establish monitoring mechanisms for policy compliance and foster strong coordination with Government of India agencies that are regulating information and cyber security practices.
- Establish and nurture strong partnerships with industry partners, academia, think tanks, online cyber security communities, and practitioners to proactively stay alert on evolving and emerging trends, standards and practices in information and cyber security.
- Establish information dissemination practice that comprises of outreach programmes and awareness workshops for citizens on protection from cybercrimes and maintaining cyber hygiene.

3. Objectives of the ICS Policy

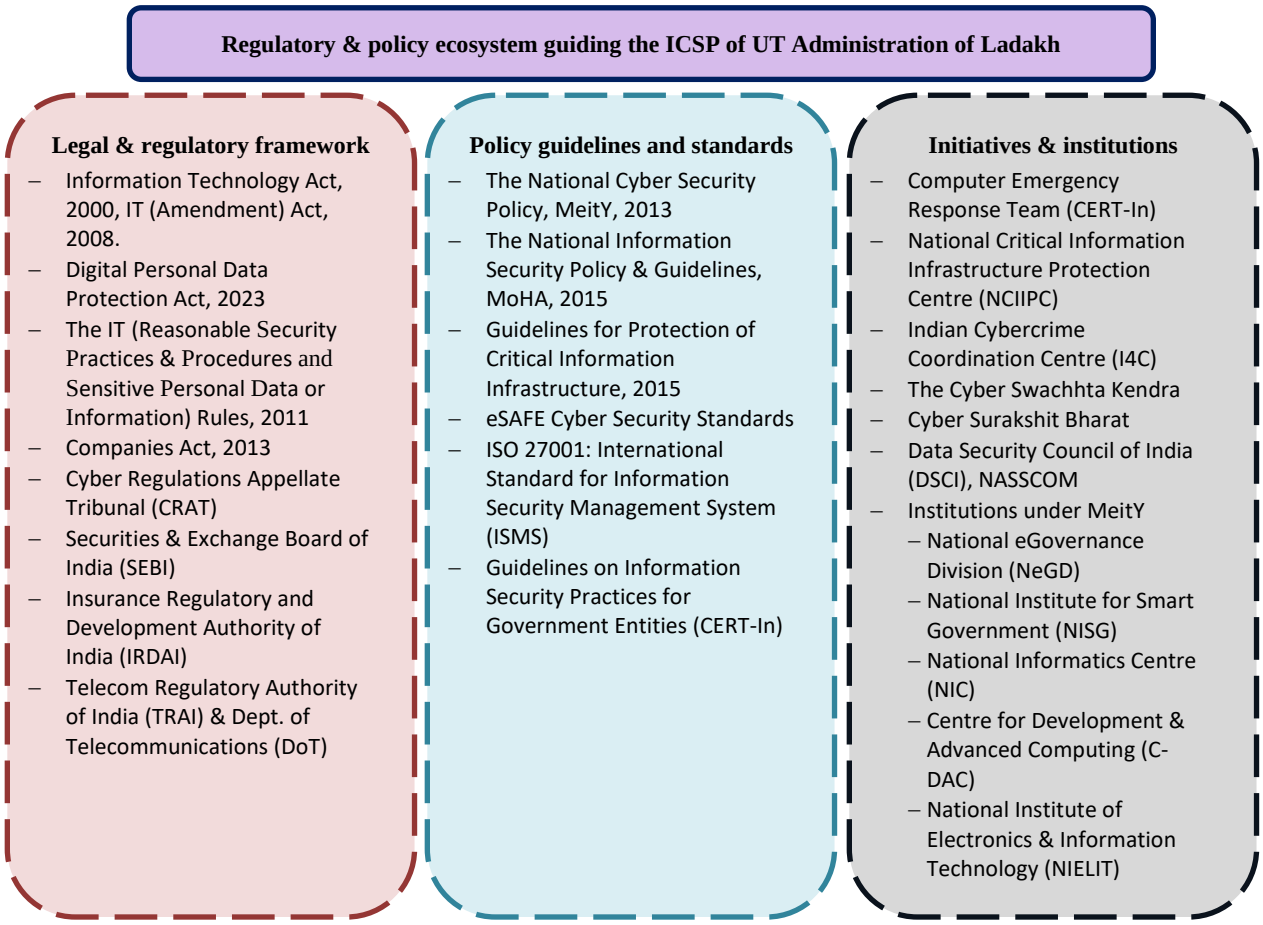
This policy aims to protect and make the CII and IT resources of the Government of UT of Ladakh accessible and readily available to the employees and legitimate users supporting the UT Administration of Ladakh. The deployment of any IT resources is understood to be in support of the endeavours, initiatives, governance, and other policies, of the UT Administration of Ladakh and prevent their access to users without legitimate access and other such unintended and unwanted users.

It is imperative that the usage of information assets, IT infrastructure and IT resources provided by the UT Administration of Ladakh, is after a deemed agreement, approval and acceptance of the user to the governance and applicability of this policy over all the activities involving the IT assets contextually referenced here. This Information and the Cyber Security Policy (ICSP) and is established with the intent to achieve the following objectives.

1. To make available the guidelines for departments, organizations, partners and vendor organization, Governments of other states, UTs and the Central Government, policy makers, consultants, experts, employees, and ex-employees extending continued support to the UT Administration of Ladakh and the citizens of the UT and the country in general, on the Policy of the UT on Information Security.
2. To build awareness and visibility to the organizations, departments, partners and vendor organizations, consultants and affiliated service providers, other state governments and centrally governed bodies, regulatory bodies on the Information and Cyber Security Policy followed by the UT Administration of Ladakh.
3. To establish, scope and define boundaries, rules and restrictions that are applicable when dealing with the information and data assets that belong to the UT of Ladakh.
4. To define the Information Security framework along the operational boundaries of its functions and departments, corporations, and establishments under the operational ecosystem of the UT Administration of Ladakh.
5. To identify and lay emphasis on securing the information, data and related assets owned by the UT Administration of Ladakh.
6. To identify, connect and integrate the criteria and assertions that relate to the information security aspects of any establishment operating in UT of Ladakh.
7. To establish and ensure the completeness and robustness of the information security framework for the UT Administration of Ladakh, covering the scope and width of the operations across all departments, functions, enterprises, offices and affiliated services.
8. To demonstrate the scope and coverage of the UT Administration of Ladakh along with its benchmarked references to national and international standards that govern the mandatory elements that constitute and define the standard information and cyber security requirements for compliance as adapted by the global and national governance bodies and industries and establishments dealing with vulnerable information and data assets.
9. To declare loud and clear the dependencies and alignment with the information and cyber security framework as an important part of the digital transformation being undertaken by the UT Administration of Ladakh.
10. To demonstrate the transitioning and transformation of its governance and operations to increasingly digitalized and data driven business transactions in a secure manner.
11. To lay emphasis on the emerging operational models leading to data analytics, an accelerated decision making, automation and visualized operations alerting the stakeholders at all levels including the general citizens about the sensitivities involved and the necessary precautions that are consequential to the information security framework that is incorporated into the governance and administrative framework of the UT Administration of Ladakh.

4. Regulatory Framework Guiding the ICS Policy of Ladakh

The Information & Cyber Security Policy (ICSP) of Ladakh aligns itself with the regulatory, policy and standard guidelines issued by the Government of India. The policy also examines other information and cyber security guidelines developed by select states to allow for comparison and improvement. Most of the recommendations and guidelines for developing the ICSP and standard operating procedures are influenced by these laws and frameworks.



5. Scope & Applicability of the ICS Policy

This policy is aligned with the secure usage of IT Resources from an end user's perspective. This policy is applicable to all employees of the UT Administration of Ladakh and those engaged in activities requiring and enabling legitimate access to the IT Resources of the UT Administrationof Ladakh directly or indirectly with an intent to facilitate, fulfil the tasks in support, assistance and enabling the cause of the UT Administration of Ladakh.

5.1. Mechanism to deploy the ICSP

This UT Administration of Ladakh will ensure the applicability of the policy across all its institutions and process that are dependent on any IT infrastructure and resources. The ICSP will be deployed through the following activities.

- Incorporating the information security framework with administrative, operational, technical, and assurance activities by integrating and carefully sequencing the information security tasks with the

business processes and services of the UT Administration of Ladakh and its functions, departments, consultants, employees, partners, and affiliates, enterprises, and retainers, is committed to deliver.

- Building familiarity and increasing the efficiency to provide secure service delivery through awareness building amongst the employees of the establishment, its functions, departments, affiliates, personnel from its enterprise entities, consultants and retainers, on this policy, the principles stated by this policy.
- Establishing the process controls that protect the information and data assets including electronic data, and personal data, of the Government across the UT of Ladakh and its functions, through periodic risk assessments and mitigation of the risk identified through sophisticated and effective means.
- Identifying the risk and vulnerabilities associated with the second party and third-party service providers and mitigating the same through effective rules of engagement conforming and confirming to confidentiality, completeness, accuracy, availability and integrity, materiality, reliability, efficiency and effectiveness and compliance to the data protection and privacy requirements.
- Ensuring that the rules of engagement are applicable not just during the period of service provision but for a time period into the future until which the impact of a vulnerability can be felt, up-to several years or a couple of decades, if required, after completing the engagement, fulfilling the regulatory and legal requirements including but not limited to non-disclosure, confidentiality and non-compete clauses amongst many.
- Continuing the improvements in the risk and vulnerability management and mitigation, strengthening the applicable controls from time to time with sophistication and robustness, addressing emerging challenges and threats from within the UT of Ladakh, within the country and outside including neighbouring countries and global hackers and intruders.

5.2. Deactivation of the ICSP

This policy deactivation may be authorized by the Union Government ruling highlighting the reasons for its deactivation. The UT Administration of Ladakh may locally decide to supersede this policy through a more sophisticated, far reaching, and overarching policy that includes the guidelines of this policy framework. Otherwise, once the authorization by the UT Administration of Ladakh is done the policy remains effective, valid and survives though all changes impacting the initiatives, Projects and business tasks of the UT Administration of Ladakh and all its functionaries. However, the ICSP will be reviewed every **3 years** and updated with necessary changes and even suggest a course change from its earlier version.

Organization(s) or individuals not aligned to the provisions of this policy would be required to justify their intent and inability or constraints and challenges in adhering to this policy. An alternative mechanism might be considered which can effectively protect the interest of the UT Administration of Ladakh in securing its Information Security assets and IT resources across the jurisdiction. In any case organizations or individuals unable to protect the interest or align with the policy would be deactivated with immediate effect upon the direction and decision of the authorized designates at the UT Administration of Ladakh.

5.3. ICS Policy Framework of Ladakh

To establish a resilient information security practice and a sustainable cyber space, the UT Administration of Ladakh's ICSP framework is built around the following 5 key components.

5.3.1. ICS compliance, controls & Audit

The ICSP framework, based on the vulnerabilities, threats and risks to the CII and its resources, should put in place necessary guidelines to develop standard operating procedures to protect IT assets of an organisation. The ICSP guidelines for developing the SOPs should discuss network and infrastructure security, identity and access management, physical security, application security, data security, personal security, threat & vulnerability management, security monitoring & incident management, security audit and testing, business continuity & disaster recovery and continuous monitoring and improvement. To protect the CII and ensure continuous monitoring of compliance and management of IT assets a separate Security Operations Centre and Network Operations Centre is proposed.

5.3.2. Institutional framework for implementation

The component highlights the institutional framework required at the UT level for implementing the ICSP. These institutional arrangements will focus on strategically guiding the implementation of ICSP, oversight, monitoring and enforcement of compliance & audit requirements under the ICSP, engaging the required workforce for implementing the ICSP, coordinating with department on their ICS practices and provide forecasts and alerts on cyber risks and best practices, establishment of cyber forensics cell in collaboration with the police department, organize outreach programmes on ICS and finally be responsible for building the capacity, skill and competency of the government officers on information and cyber security.

5.3.3. Capacity building

Both public and private sectors need to have a general awareness of cyber security practices and cyber hygiene to control cybercrime. The ICSP proposes a comprehensive capacity building plan that covers awareness building, training and skilling of officers, orientations on application ICS in emerging technologies, create a cadre of ICS professionals within the state of Ladakh, build capabilities on cyber forensics and make provisions available for certification in ICS domain. The ICSP institutional arrangements will also target and utilize MeitY's schemes on capacity building in information and cyber security like Information Security Education and Awareness (ISEA), Cyber Surakshit Bharat by MeitY etc.

5.3.4. Outreach

As part of the outreach programme the UT will focus on nurturing strong partnerships with industry, academia, think tanks and online communities to access SMEs both of national and international repute, undertake research and development on ICS, stay updated on ICS best practices and applications and create partners for implementation. The outreach activities will also focus on establishing a strong information dissemination practice that will help in creating UT-wide awareness on ICS not only among Government departments and agencies but amongst all the private establishments as well as the community and citizens in general.

5.3.5. Monitoring

The monitoring responsibility of the ICSP will be with the institutional arrangements created to implement the policy. The monitoring activities would primarily focus on the information and cyber security compliance on controls suggested under the policy. The UT will have to network closely with CERT-In and NCIIPC for reporting on incident and threat management, and risk to critical information infrastructure and assets respectively. Based on the Guidelines for SOPs, the UT Administration will monitor the development of department-specific SOPs to ensure each department follows reasonable information security practices.

5.4. Coverage of the ICS Policy of Ladakh

Based on the regulatory, legal, policy and administrative frameworks established by Government of India and key standards and templates recommended by national and international information and cyber security agencies and practitioners the broad coverage of the ICS policy of Ladakh include the following components.

5.4.1. Cyber Crisis Management Plan (CCMP)

The cyber security strategy under the National Cyber Security Policy, 2013 envisages Cyber Crisis Management Plan (CCMPs) by all critical sector entities, to reduce the risk of disruption and improve the security posture. The ICSP developed for Ladak takes into consideration some of the recommendations made by the CCMP framework and should develop the guidelines for developing the SOPs.

CCMP or cyber crisis management plan would be a strategic element over and above the threat and vulnerability management, security monitoring, incident management and the security policy guidelines that govern the routine practices of information and cybersecurity framework established at UT Administration of Ladakh. CCMP adds more resilience to double the assurance and robustness through ad-hoc and specific practices that pre-empt the

cyber-attacks and threats from realizing. The ICSP Ladakh also proposes capacity building, awareness, monitoring, and outreach activities to ensure the UT is prepared when there is a cyber crisis.

CCMP at UT Administration of Ladakh would be an investment intensive sophistication focused on a non-compromise protection with additional tools and methods to sense, identify, treat and mitigate the plans of intruders and cyber terrorists with specialized skills to break the security framework to gain access or damage the information assets across the establishments. The criteria for CCMP consideration would deal with highly critical information, severe economic impact, critical impact on the governance, people, and the general and information assets belonging to UTGL. While the vulnerabilities are listed out in the threat and vulnerability management section, the CCMP would serve the critical protection needs with increased resilience to attacks like denial of service, DDOS and to with proactive approaches like identification and tracing the attack origins and honey pots, Proactive practices under CCMP may include at critical data access levels, data packet inspections at the protocol levels, encryption and 2 Factor Authentication, quarantine, following collaborative and cooperative actions as part of an international security ecosystem.

The ICSP of the UT Administration of Ladakh covers the following key mechanisms, compliance, and control aspects as part of this policy.

5.5. ICS Mechanisms Compliance and Controls

The UT of Ladakh with its new and dynamic identity and all its uniqueness in its presence and contribution to the economic growth, identity and wellbeing of its citizen and the nation in general, is committed to establish, baseline and benchmark against itself from time to time in defining and revising the needs and deploying robust framework of Information security along with the required principles, guidelines and standards as applicable for various dimensions, assertions and criteria that address the remedial requirements for risk and vulnerabilities.

Also, along with the controls, restrictions and the discipline required to protect and secure its data and information assets, the UT of Ladakh would meet the expectations of its stakeholders by meeting the information security requirements while performing to the economic growth and development in the region. Policies, Criteria and Assertions that ensure the policy robustness in defining, deploying, and completing the required scope for Information security framework. The ICSP of the UT Administration of Ladakh covers the following key mechanisms, compliance, and control aspects as part of this policy.

5.5.1. Vulnerabilities, Threats and Risks

The UT Administration of Ladakh shall gauge the wholistic relevance of digitalization across its operations and processes towards sophistication and technology enablement. This requirement does not come free of cost and opens the vulnerabilities, threats and risks by default, from cyberattacks. Therefore, UTGL technology enablement should also focus on securing the output of strategic enablement and growth.

The UT Administration of Ladakh shall upskill and enable the councils, departments, agencies and their subordinate organizations to ensure alignment with and enforcement of globally accepted standards of information security management and governance, considering their entire operational footprint as a candidate for vulnerabilities, threats and risks. This includes deployment of practices prescribed by the standards, documentation of the vulnerabilities, threats and risks mapped to the security practices in the ministry/ departments security policy, or in some other apex level document and enabling the Chief Information Security Officer (CISO) with an efficient team to stay resilient and vigilant of the gaps in the deployment and possible cyberattacks that can exploit the gaps and weaknesses.

5.5.2. Network and infrastructure security

The UT Administration of Ladakh currently has systems discretely located and serving their purposes, supporting the operations and business processes. There is no element of integration, envisaged or attempted by the state technology function to network and build an information security boundary to protect The UT Administration of Ladakh from pilferages of critical information.

An architectural structure reinforcing the information and cybersecurity blueprint, locating information in a network arrangement and other similar infrastructure security arrangements should be in place. This also includes internal and external connections to information, protocols that are used to transfer information, with robust preparedness to withstand attacks and infiltration attempts.

Such Architecture demands and ensures the specific consideration on the controls and treatment from the perspective of securing information from actors with vested interests that can damage the functioning and economic sustenance of the governance system in UT of Ladakh.

5.5.3. Identity and access management

UT Administration of Ladakh would protect its sensitivity and critical information from those are not connected directly or indirectly with its operations and business processes. Accordingly, UT Administration of Ladakh would identify, define, and restrict the access privileges of its officials, staff, and administration to identified, authorized, designated or otherwise permitted individuals.

UT Administration of Ladakh would be clear with an emphatic answer to the question of providing access to individuals who contribute to the continued positive performance of the Ut Government, and those who are not authorized and do not need access. The ability of an individual or group of users to access and perform a set of operations on the said information is identified, authorized, and enabled. Access to third party service providers and external SMEs may require a temporary consideration with no access to intellectual property and sensitive information of the UT Government.

This is an important consideration in comparison with the regular privileged access holders who manage the projects and operations on a day-to-day basis. UT Administration of Ladakh shall have a robust mechanism in place to restrict the misuse of identities, and eliminate ad-hoc, unauthorized access from vested interests that can negatively impact the Government functioning.

5.5.4. Physical security

The UT Administration of Ladakh shall establish the physical security of the information assets as a first level of defence for Information and Cybersecurity assets. Only individuals who are authorized to access, process, handle, work or otherwise deal with the UT Administration of Ladakh's information assets including data, shall be authorized to enter the premises. An entry is made into the logs automatically through biometric or and/or access cards as a routine exercise to identify an individual's presence in the vicinity of identified information assets.

UT Administration of Ladakh will identify all such touch points from where information assets can be accessed physically. This also includes portable devices which can defeat the traditional physical screenings of individuals and create an opportunity for data and information theft. The government will also identify all such physical threats including those which can be orchestrated with other mal practices to escape with the information assets without leaving a log or footprint to trace the vulnerability to the associated damage, theft, loss and/or adverse impact.

5.5.5. Application Security

UT Administration of Ladakh will ensure that the applications deployed across its operations carrying out various transactions with the other establishments both within and outside the government are secure enough to protect information as it is processed, transferred or stored during the application lifecycle.

Based on the characteristics of applications and its accessibility to the public domain and the ensuing data availability without restriction, could expose the application adversely impacting its reliability. These variations in the security parameters at various levels of the architecture expose the information processed, stored, accessed, transacted through these applications to increased vulnerability. An assurance of information security shall be ascertained by UT Administration while procuring any application from an OEM and ensure the liability ownership by the vendor if any exposure is found or has impacted the UT Government's operations through the weaknesses with the application.

5.5.6. Data Security

UT Administration of Ladakh shall establish the hierarchical classification of data through various levels from critical, sensitive to non-critical and published levels of accessibility and availability. UT Administration of Ladakh will establish controls to ensure that the processing, handling, analysing and presenting operational, process, analytical and conclusive data shall go through authorised channels and accessibility controls.

While moving from a paper-based data base to a digitalised database, one of the first critical controls that emerges out and build increasing resilience and security of the data coming out from its operations and processes. A wrong group or individual gaining access to UT Administration data can take advantage and violate the confidentiality and privacy that UT Administration of Ladakh has maintained while carefully carrying out any such strategically significant initiatives.

5.5.7. Personal Security

The security of its employees and third-party service providers is paramount for UT Administration of Ladakh. Accordingly, UT Administration would strengthen the current security proactively with growing needs of multipoint security checks, increasing number of employees and evolving threats from geopolitical, natural, technological, fire, electrical, terrorist attacks, human initiated and such potential threats. The security establishment of the Government will work to eliminate insider and external security breaches. The UT Administration will ensure robust security mechanism including mock fire drills, inspection of fire stations and firefighting infrastructure, health of transformers and electrical substations, electrical and network cabling systems to identify and neutralize threats to the employees of the UT Administration and authorized staff of the third-party service providers, working on the information assets, and the information assets belonging to the UT establishments.

5.5.8. Threat & Vulnerability Management

The UT Administration of Ladakh would enable the information and cybersecurity establishment to identify the emerging threats including intrusion from ransomware and malware, web application attacks, denial of services, botnets, spamming, phishing, insider threats, data breaches, manipulations and theft, to mention a few. These can compromise the organizational security infrastructure causing damage to the information and cybersecurity assets.

The UT Administration of Ladakh would ensure that the threat and vulnerability management practices are suitable to the changing threat intensities, evolving capabilities and sophistication, to handle and mitigate the ensuing threat efficiently. Threat and vulnerability management is the heart of the UTGL information and cybersecurity framework which is engaged in managing the security of the information assets and at the same time protecting them from emerging threats and vulnerabilities.

5.5.9. Security Monitoring & Incident Management

Incident Management at ICSP policy would focus on the SLAs (Service Level Agreements) of the response time to an incident reporting. This is to ensure that in an eventuality of a security threat realizing, the time to respond is within the established timelines and the root cause analysis of the cyber security incident is carried out correctly. The resolution for the incident is timed well and complete to close the gaps that have led to the incident. Security Monitoring is routine check-up activities, monitoring the trends and spikes in the tasks and activities, including transfers of information, encryption and end user protection practices amongst other dynamic daily routines of employee engagement.

5.5.10. Security audit and testing

Periodic audits, reviews and regular testing of security equipment across the establishments of the UT would be carried out periodically to ensure conformance and compliance to the established security measures. Compliance to security policy, guidelines, controls, monitoring of threats and vulnerabilities, logging, DR drills, and other security practices address various elements of the information and cybersecurity framework. Tests like vulnerability and penetration tests would be conducted to identify and block unauthorized individuals, intruders, cyber attackers trying to gain illegitimate access to the network infrastructure. Security audits, testing and reviews would be conducted on a continuous basis to check for conformance to these and other security measures deployed by UTGL information and cybersecurity establishment.

5.5.11. Business continuity & Disaster Recovery

The UT Administration of Ladakh realizes that operational Business Continuity is the backbone for the sustenance and seamless performance of governance supported by a highly dependable IT infrastructure. The UT Administration would segregate critical functions whose data is backed up periodically and in the event of an unforeseen stoppages of ant site, any designated UT establishments can run the office and transactions from an alternate site.

The backup, cold and hot site for alternate operational continuity is usually an independent function that is highly recommended by global security professionals. Availability of classified and critical information, continuity of critical operations and facility followed by access for employees to perform their official dispositions, are the critical areas of focus from a Business Continuity and Disaster recovery point of view. Establishment of with RPO (Recovery Point Objective) and RTO (Recovery Time Objective) is an important control that UT Administration of Ladakh has to consider as an important control for Disaster recovery.

5.5.12. Continuous monitoring and improvement

The UT Administration of Ladakh will be vigilant on the changing landscape of sophistication and enablement. The Technology landscape is up for newer sophistication and tools for accelerating operations and processes. However, with the enablement of technology-sophistication is emerging the threat to the security of the information and cybersecurity assets. The UT Administration of Ladakh shall ensure that continuous monitoring of the mechanisms and security framework that has been deployed is carried out at an optimized periodicity to make it strategic and effective. Some of the important areas that the monitoring has to focus on are Physical Security, Network Security, Business Continuity, DR, Incident Management, Vulnerability, Threat and Risk. This will enable the UT Administration of Ladakh with not just the protection of the critical information infrastructure but also the necessary upgrades and preparedness to newer threats and along with adding more efficiency to the operational ecosystem.

5.5.13. Guidelines for developing Standard Operating Procedures (SOPs)

Based on the cyber security mechanisms required, compliances and controls required, the ICSP should put in place a set of guidelines that will help government departments and other agencies to develop their own standard operating procedures (SOPs). The ICSP aims at proactively establishing these guidelines for SOPs based on policies, regulations and national guidelines on information security and international standards like ISO 27001.

The guidelines will be shared by the Information & Cyber Security Unit within 60 days of publishing this gazette notification. The guidelines should broadly cover the following.

1. Incident Management
2. Data Back Up
3. Vulnerability Management
4. User Access
5. Logging and Monitoring
6. IT Asset Management and Disposal

7. Change Management
8. Web Application Security
9. Physical Security
10. Bring Your Own Device BYOD
11. End User Protection
12. Network Security
13. BCP & Disaster Recovery plan
14. ICS Risk & Compliance Management
15. Human Resources Security
16. IT Acceptable Use
17. Third Party Risk Management
18. Data Classification
19. Information Transfer
20. IT Secure System Development
21. Clean-Desk
22. IPS/IDS deployment
23. Network-Hardening
24. Encryption and Passwords
25. Patch Management
26. Server Virtualization

5.6. Institutional Framework for ICSP Implementation

The overall institutional arrangements proposed for implementing the ICSP of Ladakh would take into consideration the following key aspects.

1. Vision and strategic direction for ICSP
2. UT level coordination and implementation monitoring
3. Implementation at the department level
4. Promoting cyber forensics
5. Capacity building & outreach

The institutional arrangements will be placed at various levels starting from the UT level to the department level.

5.6.1. Information & Cyber Security Steering Committee (ICSSC)

At the State Level, to provide the strategic vision as well as direction for implementing the ICSP the UT Administration of Ladakh will establish an Information & Cyber Security Steering Committee (ICSSC). This committee in addition to providing strategic direction, will make provision for necessary budget and finances required for implementing the ICSP, review implementation progress and release directives to stakeholders on compliance requirements. The composition of the ICSSE would include the following personnel.

1. Lieutenant Governor, UT of Ladakh (Chairman)
2. Advisor, UT of Ladakh (Advisor)
3. Administrative Secretary, General Administration Department (Member)
4. Administrative Secretary, Department of Home (Member)
5. Representative from Armed Forces (Member)
6. Secretary IT Department, UT of Ladakh (Convenor)

5.6.2. Information & Cyber Security Unit

The responsibility of coordination with various departments, government agencies and administration at the district level will be with the Information and Cyber Security Unit (ICSU) established at the IT Department with the Secretary IT Department as its Chairman. All the security operations at the ICSU will be led by a designated officer who is the Chief Information Security Officer (CISO) of the UT. The CISO of the UT of Ladakh will be supported by a Deputy CISO and Information Security Officers. This team will also control the Security

Operations Centre (SOC) of the UT and coordinate with designated Information Security Officers (ISO) at the district & the department level.

5.6.3. District Information Security Officer

At the district Level, the district administration of Leh and Kargil along with the Districts & Ladakh Autonomous Hill Development Council will be supported by a District Information Security Officer's (DISO) who is responsible for maintaining the security of systems at the district offices.

5.6.4. Information Security Officer

At the Department level each department will have a dedicated information security officer who will in charge of security of critical information assets of the department. The ISOs will coordinate with the ICSU for incident reporting, security audit and be responsible for security compliance and maintaining security controls.

5.6.5. Cyber Forensics Cell

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it. The Cyber Forensics Cell will closely work with the Special Investigation Team in-charge of cyber security located at the office of the Additional Director General of Police, Ladakh. The Cyber Forensics Cell will be manned by an information security officer and will also support the CISO on forensic matters.

5.6.6. Cyber Security Grievance Help Desk

The Information & Cyber Security information dissemination, information support and redressal of grievances will be handled by the special help desk create for all the stakeholders. The help desk will be manned by 2 resources and operate based on the specific SOPs that would be developed for resolving issues pertaining to information and cyber security.

5.6.7. Network Operations Centre Team

The Networks Operations Centre (NOC) of Ladakh is established with the purpose of there should be dedicated NOC with strong team to monitor, maintain, manage, and secure the organization data. Larger, medium to smaller organizations or Master Services Providers (MSPs) across Ladakh can connect to the NOC team. The NOC can help them manage complex IT infrastructures to secure their data from the unauthorized persons.

5.6.8. Security Operations Centre Team

A Security Operations Center (SOC), is a critical centralized unit within an organisation responsible for monitoring, detecting, investigating, responding, and preventing its security posture and threat 24 x 7, which is managed by the IT security or InfoSec team. Thus, SOC acts as a hub, ensuring an organization's IT network always operates securely, round the clock.

The SOC is a command center that monitors an organization's IT infrastructure. This includes Websites, Databases, Servers, Applications, Networks, Desktops, Data Centers, Endpoints.
A SOC is staffed by IT professionals with expertise in information security. They will monitor, analyse, and protect an organization from cyber-attacks (DDOS, SQL Injection, Ransome Virus, Trojan attacks, Dark Hacking, Phishing attack etc.)

5.6.9. Establishing the Network Operations Centre (NOC)

The UT Administration of Ladakh has proposed establishing a Software Defined Wide-Area Network (SDWAN), a Next Generation SWAN network for Ladakh. It will act as the backbone network for voice, video and data communications for the entire UT covering all Government offices. The UT Administration of Ladakh has

approved the Scheme for establishing Statewide Area Networks (SWANs) In UT Ladakh up to around 2 Districts, covering 31 blocks and 193 Gram Panchayats. All Government offices shall be connected to the last mile offices on a secure platform and the UT Administration of Ladakh is planning to complete the project by the end of March 2024. Some of the major benefits that the proposed SDWAN include:

- SWAN would help in ensuring maximum uptime for VSAT at Gram Panchayats.
- 24x7 Hotline availability through IP telephony for emergencies/Disaster Management.
- Service availability with multi-ISP/redundancy of Links in case of natural calamity/disaster through SDWAN technology till last mile.
- Secured and encrypted communication across state/district/block headquarters & villages & Gram Panchayats
- Wi-fi services can be extended at GPs leveraging SWAN/SDWAN device.

To successfully implement the ICSP the UT Administration of Ladakh proposes to set up a Network Operations Center (NOC) at the State Data Centre. Some compelling reasons for establishing a NOC ate listed below.

1. ***New threats*:** Currently UT Administration of Ladakh (UTGL) is dependent on a network which is not scalable when it comes to its own needs. The network services and support facilities are not directly mapped to the needs of UTGL as UTGL itself is an ad hoc user of the facility. This increases the vulnerability of the UTGL operations to newer and emerging threats that UTGL may not be able to monitor itself. New threats like DDOS or DOS, researchers from the security domain have identified newer tactics that the attackers use through social engineering, data theft, ransomware, and such attacks. To add capability and skillset to monitor, maintain and prepare to address the innovative threats and high vulnerabilities, UTGL would have to look outside the limited dependency it is availing from the service provider. A sophisticated UTGL NOC would mean firstly autonomous thinking to measure and assess the network services and support needs of its operations and processes across the establishments. It enables the UTGL with a new capability to play a back-up role with an oversight on balancing and optimizing the network resource needs across its operations and establishments by itself. This enables UTGL to be sure of and proactively identify and thwart the attacks from increasingly intelligent information and cybersecurity hackers.
2. ***Setting up own SDWAN***: UTGL is currently dependent on the private network service providers. While the operations of UTGL are scaling up on a day-to-day basis, UTGL would not be keen to see a day where the services availed are hitting a cap on the availability due to increased demand supply imbalance. UTGL shall endeavour to move its dependency to its own SDWAN with scalability and sophistication to reach and resolve the corners and concerns of their establishments across the UTGL region.
3. ***Greenfield Establishment***: UTGL is right at the mouth of a gigantic growth opportunity being a greenfield tech savvy establishment starting all over from the scratch with a hunger and vision to gain autonomy from network dependency, develop into an epicentre capable to serve the several public, private and discrete buyers to avail and gain advantage of the NOC that the UTGL intends to build.
4. ***Trend setting and futuristic***: The envisaged UTGL NOC would be a first of its kind in the region with capability to meet the centralized network services and support requirements not just for running its operations and process needs but also to promote and support sophistication and capabilities to the interested businesses and service seekers. UTGL may take advantage of the emerging network technology aspects combined with the high efficiency security support mechanism that it intends to set up in the UT of L. An integrated NSOC could be a highly equipped entity with the capability to meet the overarching needs of the network operations working in tandem with the security operational aspects run from a high potential establishment.
5. ***Creating an accessible and efficient Service center***: The proposed NOC will provide a network as a service for other institutions which can fulfill their business needs. These institutions may include but not limit to:
    a. *Defense establishment*: to enhance and add more efficiency to their network capacity.
    b. *Border Roads Organization*: From a network provider the envisioned capacity of UTGL network resources would support BRO to rethink and enhance their requirement that subsequently impact their network needs exhaustively to add more sophistication to their current services and operations. That is to say that BRO would add more capability by a possible outsourcing of their Network requirements to the envisioned UTGL NOC.

c. *Current universities and educational institutions*: Educational institutions would get immensely benefitted from the UTGL NOC by becoming users of this redundant resource to their advantage by accelerating their processes and business needs with the sophistication possible from the UTGL NOC. New universities, medical colleges and other educational establishments may be keen to take advantage of the UTGL NOC as an opportunity of the sunrise.
d. *New Businesses & MSMEs*: UTGL NOC can be very attractive proposition for new businesses and MSMEs from the private sector to avail services from the new generation NOC. UTGL would thus be contributing not just to the technology enhancements but also to the economic growth of the UT of Ladakh by attracting businesses to a favorable and friendly destination.
e. *Secure Network*: A secure network from an established and sophisticated UTGL NOC would mean clean technology availability to the public of Ladakh in general to avail and upgrade their technology needs to newer and innovative services leading the entrepreneurial think tank getting bigger and brighter in the vicinity.

5.6.10. Establishing the Security Operations Centre (SOC)

Accordingly, to put more emphasis on the security aspects that define the purpose of a UTGL-SOC as envisaged, the need for dedicated UTGL Security Operations Centres (SOC) is crucial, and this is irrespective of the size or domain of the establishments integrated under the governance of the UTGL. A UTGL-SOC is a critical centralized unit within UTGL vested with the responsibility for monitoring, detecting, investigating, responding and preventing its security posture and threat 24 x 7, managed by the Information Security team. Thus, UTGL-SOC acts as a hub, ensuring UTGL's IT network always operates securely, round the clock.

UTGL-SOC is a command centre that monitors its IT infrastructure including their Websites, Databases, Servers, Applications, Networks, Desktops, Data Centres, Endpoints supporting, serving and servicing the UTGL operations. The UTGL-SOC would be staffed by IT professionals with expertise in information security to monitor, analyse, and protect UTGL and it support systems from cyber-attacks (DDOS, SQL Injection, Ransome Virus, Trojan attacks, Dark Hacking, Phishing attack etc.) The UTGL Security Operations Centre (UTGL-SOC) is important because it:

- Reduces the cost of data breach for UTGL
- Get faster response by real-time monitoring by its own team of experts
- Reduce cybersecurity risks in the long run by proactive and highly resilient governance of its SOC
- Provide real-time network updates for analysis and approach to IT operations
- Provide more visibility into systems for robust integration without caveats
- Create alerts when unexpected behaviour is detected
- Develop the capability to consume and leverage threat intelligence
- Collect as much data and context as possible
- Prioritize incidents for preparedness and prevention

UTGL-SOC would utilize a combination of the right tools and the right skillset to build, operate and maintain a security architecture within UTGL using advanced technologies. The UTGL-SOC's primary function is to monitor & protect UTGL's IT assets, IPR, personnel data, and operations and business systems and, thus, safeguard the integrity that UTGL intends to build as an emerging governance centre in the region.

In addition, the UTGL-SOC support engineers deploy a comprehensive cyber security strategy that encapsulates activity on servers, networks, applications, endpoint devices, websites, and other critical internal systems to identify and detect the vulnerability and defend most effectively to dissolve it. The key responsibilities of UTGL-SOC will include the following.

1. *24/7Monitoring*: Proactive, around-the-clock monitoring of the organization's network ecosystem for threat and incident response.
2. *Log Monitoring*: Analysis of logs, network traffic patterns, and other external data sources to identify potential vulnerabilities.

3. *Threat Intelligence*: Threat intelligence can assist the SOC team in making the right decisions to prevent an attack and decrease the time it takes to discover the threat in action.
4. *Root Cause Analysis*: This is a systematic analysis & process to define, measure, analyse, improve, control and document the root cause of an incident to ensure the incident is not repeated.
5. *Rules/Policies Creation*: Create consistent policies that integrate best practices and organizational requirements for monitoring, incident response, reporting, and staffing.
6. *Assessment & Compliance Management*: This defines auditing procedures for organizations to securely manage data to protect their interests and privacy and ensure the systems for compliance with regulations which may be issued by an organization, industry, or governing bodies. Examples of these regulations include GDPR, HIPAA, and PCI DSS etc.
7. *Device Management*: This acts like the hub managing all of the organization's IT infrastructure, including networks, devices, appliances, tools and databases, and other assets.

5.7. Capacity Building Plan under ICSP

Digital transformation is the integration of digital technology into all areas of a business, fundamentally changing how you operate and deliver value to customers. Governments need to subscribe to the fact that information technology and digital solutions are here to stay, and governments must work towards constantly improving their capabilities in using technology and that transformation can be relative in government organizations based on their current eGovernance maturity.

Managing the quantum of services to be delivered, financial and budgetary limitations and priorities that government wrestle with, living up to the expectations of the people, opening up to public scrutiny and stakeholder acceptability coupled with inadequate capabilities and resistance to change can impact the outcomes that government desire. It can be safely said that if governments do not adapt to the fast pace set by technology, they are bound to fail.

5.7.1. Capacity Building & Institutional Competence for Implementing ICSP

Today, we are more interconnected than ever before and overall reliance on the Internet continues to increase. Unfortunately, in this environment cyber-attacks occur rapidly and spread across the globe in minutes without regard to borders, geography, or national jurisdictions. With countries resorting to digital warfare and hackers targeting business organizations and government processes, State and UTs within India must create awareness, build capacities and become resilient organizations that can ward off any imminent cyber threats or risks. India has a robust regulatory, policy frameworks and institutions that are promoting cyber security and hygiene and provide a very conducive and enabling environment for building capacities in information and cyber security.

The program design of the capacity building and training plan would ensure that departmental functionaries are made aware of cybersecurity practices, ICSP of Ladakh, other cyber law acts and policies in India, cyber forensics, cybercrime and demonstrate various tools available to keep a check on, evaluate and identify such attacks in the future.

The implementation and monitoring of the capacity building plan for the UT Administration of Ladakh under the ICSP will be the responsibility of Information and Cyber Security Unit (ICSU) established at the IT Department of UT. The Capacity Building Plan under the ICSP of Ladakh identifies a spectrum of capacity building interventions, strategically selected for building the necessary skills and capacities in the Government. These interventions include the following.

1. Awareness building workshops and programmes
2. Capacity Building through training and skilling
3. Train the Trainers (TTT)
4. Develop capabilities on cyber forensics
5. Create certified professionals in Government on ICS

5.7.2. Awareness Building workshops and programmes

These workshops and programmes are aimed at creating general awareness on information and cyber security. These programmes are not limited to ICT functionaries in the government but will include all the stakeholders who need awareness like government functionaries at all levels and in all organizations and institutions, Citizens, Civil Society Organizations (CSOs), Public Sector Undertakings, Banks and Financial Institutions, Markets, Private Businesses, Schools & Educational Institutions, Universities, Community-Based Organizations (CBOs) and Social Capital working at the grassroots.

5.7.3. Capacity Building through Training and Skilling

This activity will constitute training and skilling programmes on Information and Cyber Security (ICS). Appropriate training courses will be developed for government functionaries on various aspects of ICS. Depending upon the roles and responsibilities allocated to the officers at senior, middle and entry level roles the UT Administration of Ladakh for the purpose of training and skilling will broadly cater to the following 4 groups.

S.No	Management level	Functional Responsibility
1.	Leadership	**Leaders** strategizing and planning ICT for the UT
2.	Senior management	**Champions** heading and managing ICT in departments
3.	Middle management	ICT programme **Managers** implementation and execution
4.	Specialised support	**Executives** designing, implementing, and monitoring ICT projects

The training and skilling programmes will contain conceptual lectures, practical exercises, demonstrations, case-study based learning, roleplays, and tool-based learning.

5.7.4. Customized Training Programmes for stakeholders

This activity will constitute creatin customised training programmes for various stakeholders by detailing their roles and responsibilities vis-à-vis information and cyber security practices. These stakeholders not only include Government departments but also PSUs, banks, telecom companies and other key industries and citizen-based organizations that have critical information infrastructure.

5.7.5. Train the Trainers (TTT)

The Train the Trainers' programmes will focus on creating a cadre or pool of trainers on information and cyber security. The participants for such programmes will be handpicked by the UT Administration of Ladakh who have proven skills in implementing IT projects in the government. They will include officers from all levels of the government who will purposefully trained to become trainers who will further develop the capacities in their respective departments or organizations. These would include Information Security Officers (ISOs), ICT executives and CISOs and Deputy CISOs.

5.7.6. Develop Capacities in Government on Cyber Forensics

The Cyber forensics programme will be specifically developed however not limited to for the investigative agencies and judiciary in the UT of Ladakh. In the civil and criminal justice system, computer forensics helps ensure the integrity of digital evidence presented in court cases. As computers and other data-collecting devices are used more frequently in every aspect of life, digital evidence - and the forensic process used to collect, preserve, and investigate it - has become more important in solving crimes and other legal issues. Digital evidence is not just useful in solving digital-world crimes, such as data theft, network breaches and illicit online transactions. It is also used to solve physical-world crimes, such as burglary, assault, hit-and-run accidents, and murder. Hence the focus of capacity building on cyber forensics would be to create necessary skills and competency among officers on computer forensics covering concepts such as database forensics, email forensics, malware forensics, memory forensics, mobile forensics, network forensics etc.

5.7.7. Create Certified Professionals in Government on ICS

NASSCOM, Industry 4.0 and World Economic Forum all recommend organizations to be future ready with necessary competencies in IT/ ITeS Sector which includes information and cyber security. Today these is a robust Cyber Security skills ecosystem in the country that allow for creating expertise and competency in ICS domain. The UT Administration of Ladakh will encourage officers handling critical information infrastructure and working in the ICT environment undertake specialised certificate programmes on ICS. Some courses proposed include the following.

1. ISO 27001 Certification
2. Certificate on Data Privacy Compliance
3. Certified Information Systems Security professional (CISSP) Certification
4. Certified Information Security Manager (CISM) Certification and
5. Certified Information Systems Auditor (CISA) Certification

The above courses will allow the UT of Ladakh to have internal capabilities and competencies to handle all information and cyber security compliance requirements.

5.8. Outreach Programmes under ICSP

The outreach programme under the ICSP will be a holistic plan focussing on stakeholders. Specific interventions will be planned annually to ensure that sufficient awareness is created on information and cyber security. Key interventions of UT Administration of Ladakh's outreach programme include the following.

1. Creating gainful partnerships for combating cybercrime
2. Develop curriculum and pedagogy for academia
3. Information dissemination & citizen outreach
4. Online cyber security community of practice (COP)
5. Knowledge workshops, hackathons & meets

5.8.1. Creating strategic partnerships for combating cybercrime

UT Administration of Ladakh will network with several organizations both national and international to forge partnerships to undertake planned activities and interventions to extend the vision of ICSP. Institutions like NASSCOM, DSCI, National Institute for Smart Government (NISG), Centre for Development of Advanced Computing (C-DAC) etc., would be partners in implementing the ICSP.

The UT Administration of Ladakh will also collaborate with universities and the corporate sector for research and development. Start-ups will be encouraged to showcase their products that can be applicable to the government sector. Strategic partnerships with private sector will also be set up necessary infrastructure set-up for cyber security training, development labs, Innovation centres etc.

Broad areas of collaboration where UT Administration of Ladakh will foster partnerships will include the following.

1. Develop Information & knowledge management on ICS
2. Develop innovations for managing ICS.
3. Develop SOPs on information & cyber security.
4. Design, develop and execute training and skilling programmes on ICS.
5. Develop ICS competencies through certifications.
6. Develop eLearning (LMS) solutions and story boards on ICS.
7. Document case studies and best practices on ICS.
8. Develop pool of resources and faculty development programmes.

5.8.2. Develop Curriculum and Pedagogy for Academia

The UT Administration of Ladakh will design and develop specialised course material, curriculum, and necessary pedagogy for introducing courses on cyber security and cyber hygiene for schools, colleges, and universities in Ladakh. The ICSU established at the IT Department will collaborate with MeitY, NCERT and other educational institutions to develop such material for educational purposes.

5.8.3. Information Dissemination & Citizen Outreach

Creating awareness at the grassroots and involving strong citizen engagement is a fool proof way for the imparting digital literacy on cyber security could be hardly overestimated. Information provided by initiatives such as Indian Cybercrime Coordination Centre (I4C) and Cyber Swachhta Kendra will be made available to citizens freely. It goes far beyond enabling people to navigate the Internet; it improves citizens' awareness on cybercrime, empowers them to participate with communities online with sufficient information on cyber threats, and what is more important, serves as a tool that enables them to acquire other significant life skills. While availability of digital infrastructure will play a crucial role in bridging the existing gaps, it is equally important to build awareness on cyber security. Some of the interventions proposed for this would include the following measures.

1. Public consultations
2. Social-media posts
3. Optimal use of television & print media
4. Information sources on UT Administration websites
5. Redressal of grievances through cyber security helpline
6. Engaging social capital for mass awareness on cyber security
7. Creating of Information, education and communication material like pamphlets, flyers, posters, web announcements etc.

The Government shall also coordinate with banks, mobile companies, and financial institutions within the UT of Ladakh to improve awareness on information and cybersecurity measures that can be adopted.

5.8.4. Online cyber security Community of Practice (COP)

The focus this COP would be to bring together eGovernance enthusiasts, practitioners, government officials working on eGovernance together on to a single platform to discuss and share ideas, solutions for better implementation and service delivery. The platform created by the UT Administration of Ladakh will facilitate access to and sharing of existing and newly created knowledge on ICS. This will allow for knowledge pertaining to ICS useful to practitioners, policy makers, researchers and trainers is available in one place in a structured and easily accessible form.

5.8.5. Knowledge Workshops, Hackathons & Meets

The UT Administration of Ladakh will focus on organizing knowledge workshops on ICS. These workshops will bring together specialists, practitioners, industry partners and technology providers together to a common platform to share information., ideate on solutions for combating cyber threats and vulnerabilities. These meetings can be workshops, hackathons, expos, SME and Start-Up symposiums etc.

5.9. Implementation monitoring of ICSP

The ICSU established at the IT Department will be responsible for monitoring the implementation and sustainability of interventions proposed under the ICSP. Broadly the monitoring would include the following.

1. UT Level Monitoring of interventions proposed under the ICSP by the ICSU
2. Regular monitoring and reporting on incident & threat management to CERT-In

3. Monitoring and reporting on any risk to critical information infrastructure to NCIIPC
4. Monitoring the development of Standards and Operating Procedures at the Department Level based on ISO 27001 and guidelines provided in the ICSP by the ICSU
5. Monitoring and initiation of security audit and testing of established standards, practices and processes pertaining to ICS with the help of STQC.

By Order of the Administration of UT of Ladakh.

AMIT SHARMA
Digitally signed by AMIT SHARMA
Date: 2024.08.01 13:46:58 +05'30'

Sd/-
Amit Sharma, IAS
Administrative Secretary, IT Department, UT of Ladakh

MICHAEL MANNY DSOUZA
Digitally signed by MICHAEL MANNY DSOUZA
Date: 2024.08.01 17:25:19 +05'30'